DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
WASHINGTON, D C 20372-5120

IN REPLY REFER TO

BUMEDINST 5239.1
BUMED-09D
14 Feb 92

BUMED INSTRUCTION 5239.1

From: Chief, Bureau of Medicine Surgery

Subj: BUREAU OF MEDICINE AND SURGERY (BUMED) AUTOMATED INFORMATION SYSTEM (AIS) SECURITY PROGRAM

Ref: (a) SECNAVINST 5239.2
(b) FIRMR Chapter 201
(c) OPNAVINST 5530.14B
(d) OPNAVINST 5510.1H
(e) DoD 5200.28-STD dated Dec 85
(f) CSC-STD-002-85
(g) OPNAVINST C5510.93F (NOTAL)
(h) FIRMR Bulletin 30
(i) Title 18, United States Code, Section 1030, Fraud and Related Activity in Conjunction with Computers
(j) NAVDAC Advisory Bulletin No. 42.5 of 30 Sep 87
(k) SECNAVINST 5214.2B

Encl: (1) Definitions

1. Purpose

a. To establish and maintain the Bureau of Medicine and Surgery (BUMED) Automated Information System (AIS) Security Program per references (a) through (k).

b. To define the organizational structure to execute the BUMED AIS Security Program.

c. To provide policies to implement AIS security throughout BUMED.

d. To apply basic policy and principles of security as they relate to computer-based medical information systems which handle classified and sensitive unclassified information.

2. Cancellation. NAVMEDCOMINST 5239.1.

3. Definitions. Enclosure (1) provides definitions not contained in appendix A of reference (a).

4. Objectives. To ensure the availability of reliable information and automated support required to meet BUMED's mission by adequately protecting all supported AIS, networks, and computer resources against accidental or intentional destruction, unauthorized disclosure, denial of service, and unauthorized modification. This must be met by ensuring that physical, administrative, and operational procedures, personnel, communications, emanations, hardware, software, and data security element AIS security countermeasures are provided and are collectively adequate to protect against such events as material hazards, fire, misuse, espionage, or malicious acts. More specifically, the primary objectives of the BUMED AIS Security Program are:

a. Accuracy. All data entrusted to AIS storage and processing must be accurately maintained, i.e., remain as received from the owner or user of this information.

b. Availability. Naval Medical Department activities must develop, maintain, and test contingency plans designed to prevent loss of data or minimize periods of nonaccessibility to data stored on AISs.

c. Protection Against Disclosure. Security features available in the system software releases must be used at all times to prevent unauthorized disclosure of information.

d. Risk Management Program. Naval Medical Department activities must maintain a risk management program to provide operational procedures to prevent disclosure or modification of information and lapses in AIS support.

e. Risk Assessment. Naval Medical Department activities must implement a security program based on a risk assessment to determine how much protection is required and exists. The AIS security program must be an ongoing effort that must be reevaluated whenever changes occur in the AIS environment.

f. Security Test and Evaluation (ST&E). In support of management control reviews, a ST&E must be performed on all the computer systems by the automatic data processing security officer (ADPSO) in conjunction with appropriate automatic data processing systems security officers (ADPSSOs). The details of the ST&E must be determined upon the completion of a risk assessment. This method of internal review must be used when major changes are made to the AIS.

g. Accreditation. Six steps to achieving command accreditation on each AIS and network are:

(1) Plan of action and milestones (POA&M).

(2) Activity AIS risk assessment team charter.

(3) Risk assessment.

(4) Contingency plan.

(5) ST&E.

(6) Documentation and request for accreditation.

5. Scope

a. All naval Medical Department staff personnel must comply with this instruction.

b. Department of Defense (DoD), Department of Navy (DON), and BUMED-sponsored contractors who operate contractor-owned or BUMED-owned or controlled AIS, networks, or AIS resources on or off BUMED premises.

c. All AIS, networks, and computer resources designed, developed, or procured by naval Medical Department activities per reference (b).

d. Joint service or other AIS, networks, or computer resources operated but not owned by BUMED, when security requirements have not been specified.

e. Printing and imaging equipment or systems which are part of an AIS, connected to a network, or driven by a process control or embedded computers.

6. Policy

a. All BUMED AIS, networks, and computer resources must be protected by the continuous employment of appropriate protective measures. The policies in reference (a) apply to the following naval Medical Department activities: accreditation, life cycle management, risk management, contingency planning, user access, security implementation, interoperability, and the formal written appointment of AIS security personnel.

(1) All naval Medical Department activities operating AIS equipment must be accredited or have an interim authority to operate.

(2) BUMED (MED-09D) must approve, in writing, the authority to process classified information on any AIS equipment or any network after certification by the Naval Investigative Service Command and Naval Electronic Systems Security Engineering Center.

(3) Classified, privacy act, and sensitive data must be protected per references (a), (c), and (d).

b. All BUMED AIS, networks, and computer resources that handle classified or sensitive unclassified information must implement as a minimum, Class C2 functionality per references (e) and (f).

c. Personal computers must be protected to provide C2 level protection.

d. Non-TEMPEST approved personal computers cannot be used to process level I (classified) data. Authorization to process level I data must be specifically approved by MED-09D using TEMPEST-approved systems per reference (g). The department, division, or section head and the ADPSSO are responsible for establishing local standard operating procedures to ensure control of data and files used on personal computers (i.e., security level, privacy act infringements, integrity and efficiency aspects, and unauthorized use of DoD and DON resources).

e. Use of privately owned personal computers and personally owned software within the BUMED claimancy is strongly discouraged per reference (h) and cannot serve as the justification for sole source procurement based on hardware and software compatibility. Installation and use of privately owned personal computers or software within BUMED is only permitted with prior written permission, including a statement of BUMED nonavailability by the designated approving authority (DAA). All privately owned personal computers and software require AIS security accreditation and certification.

f. Remote access to naval Medical Department activity computers is permitted with prior written approval of the host command's security manager and ADPSO and must comply with BUMED AIS security requirements.

g. All naval Medical Department personnel and contractors employed by BUMED must have security clearances appropriate to the highest level of data handled.

h. Noncommercial software systems received as part of multiple activity distribution must be certified by the activity proliferating the system. Specifically, the project manager must provide the responsible ADPSO or ADPSSO with an AIS security certification statement certifying that the system was properly designed and that the system properly implements the appropriate functions.

i. The system administrator for any BUMED bulletin board system (BBS) must ensure that each program or file uploaded to the BBS is legitimate and free of malicious code, such as viruses or trojan horses. Unauthorized copies of commercially available software, including operating systems, cannot be uploaded to any BBS. Shareware, public domain programs, or any useful programs must be submitted to the system operator in source code. The system operator must examine and test the source code to verify the absence of malicious program logic and then compile the source code. Passwords must be used for BBS access.

j. System operators must ensure that their BBSs exhibit a warning statement before the BBS banner which in part states " ... unauthorized access to this United States Government system and software is prohibited by Title 18, United States Code, Section 1030, Fraud and Related Activity in Conjunction with Computers." per reference (i).

7. Responsibilities

a. Chief, BUMED is responsible for all AIS activities and functions, including AIS security, of naval Medical Department activities. Chief, BUMED has delegated this responsibility to the Commanding Officer, Naval Medical Data Services Center (NAVMEDATASERVCEN) as the special assistant for management information systems (MED-09D) serving as the BUMED DAA, where applicable. With specific regard to AIS security and the DON AIS security program, MED-09D must appoint the BUMED ADPSO, in writing, describing the position's responsibilities. MED-09D may delegate monitoring responsibilities to the AIS security staff, including the NAVMEDATASERVCEN detachments at Norfolk, VA and San Diego, CA. Such delegation does not reduce custodian, user, or program manager responsibility for compliance with AIS asset protection requirements.

b. BUMED ADPSO is under the administrative control of the Commanding Officer, NAVMEDATASERVCEN. The BUMED ADPSO advises the Chief, BUMED via MED-09D, on all AIS security matters and acts as the BUMED coordinator for all AIS security matters:

(1) Implements, promotes, and maintains the BUMED AIS Security Program.

(2) Conducts site inspections of naval Medical Department commands to ensure continued compliance with appropriate AIS security requirements, to maintain accreditation, and approval to operate.

(3) Maintains BUMED AIS security policy.

(4) Implements and evaluates AIS security procedures to establish policies for BUMED AISs and networks.

(5) Provides guidance to each naval Medical Department activity developing an activity AIS security plan and activity accreditation schedule (AAISSP/AAS) for BUMED approval per references (a) and (j).

(6) Recommends approval of all naval Medical Department activity AAISSP/AAS; approves individually developed systems and networks risk and threat analyses, contingency plans, ST&E plans, and plans and policy handbooks for each naval Medical Department activity.

(7) Conducts and provides information on AIS security training to all naval Medical Department activities.

(8) Provides management, technical assistance, and advice to BUMED system managers and component ADPSOs in implementing the DON AIS security program and establishing contingency and test plans which meet individual command AIS security requirements.

(9) Maintains a consolidated file of all BUMED AIS and TEMPEST security-related matters.

(10) Serves as the BUMED point of contact for external inquiries concerning AIS and TEMPEST security.

(11) Coordinates and collects information related to all AIS security incidents and submits incident reports to the Chief, BUMED, Naval Security Group (NAVSECGRU), or Naval Investigative Service Command, as appropriate. Chief, BUMED may direct that any system in violation of the BUMED AIS security program, or any system involved in a possible compromise of sensitive or classified information of sufficient magnitude, be secured from further operation.

c. BUMED Network Security Officer (NSO) is under the administrative control of MED-09D. The BUMED NSO must be appointed, in writing, for all BUMED sponsored networks. The NSO:

(1) Is responsible to the BUMED ADPSO for implementing, maintaining, and enforcing prescribed security requirements applicable to the network under their security cognizance. NSO duties, at a minimum, are in paragraph 2.3b of reference (b). External NSO appointments are the responsibility of the senior authority, command, or host computer activity.

(2) Ensures that countermeasures and requirements are included in the network design and that individual nodes of the

network comply with these countermeasures and requirements, before interfacing with the network. The security requirements must be agreed to, in writing, by the network DAA and the AIS activity connected to the network. Networks having multiple service or agency members must be accredited jointly. Network accreditation must be based on the prior accreditation of each network node.

(3) Develops and issues the standard AIS and network security procedures governing network operations.

(4) Ensures that security measures and procedures used at network modems fully support the security integrity of the network.

(5) Maintains liaison with all ADPSSOs in the network.

(6) Ensures that all required countermeasures are in place and in use.

d. Commanding Officers (COs) and Officers in Charge (OICs). As the DAA for their commands, each CO and OIC must certify that the system under their security cognizance meets, and adheres to, prescribed security requirements and standards in reference (a). Each CO and OIC must appoint, in writing, an AIS security staff with an ADPSO as a minimum. Send a copy of the command ADPSO appointment correspondence to MED-09D for retention. The CO or OIC may delegate monitoring responsibilities to the AIS security staff, if such delegation is supported by clearly stated delegation commitments and responsibilities. This delegation does not reduce custodian, user, or program manager responsibility to comply with AIS asset protection requirements. The command must take reasonable steps to understand conditions surrounding the custody, use, or development of assets, initiate appropriate actions when problems are identified, and participate in custodian, user, and developer risk assessment decisions. More specifically, the CO and OIC:

(1) Establish the asset's operational value and importance.

(2) Specify operational controls.

(3) Classify the asset and specify asset protection controls commensurate with the value of the assets being protected.

(4) Authorize access and assign custody of equipment and data to appropriate personnel.

(5) Communicate control and protection requirements to custodians and users.

(6) Monitor compliance and periodically review control and classification decisions.

(7) Ensure position descriptions for personnel assigned as the command ADPSO, ADPSSO, terminal area and assistant terminal area security officers (TASO and ATASO), and NSO define AIS security duties and responsibilities. These must be made a part of the individual Performance Appraisal Program (PAP) completed by departmental supervisors.

(8) Specific AIS security staff assignments include:

(a) The ADPSO advises the CO or OIC on all AIS security matters and acts as the command coordinator for all AIS security matters.

(b) The ADPSSO at each subordinate activity having AIS must be appointed, in writing, as ADPSSO for each system within their command. Copies of all AIS staff assignment letters must be retained in the activity's ADPSO security program file. Where span of control must not be adversely affected, a single ADPSO may be appointed to more than one specifically identified system.

(c) TASOs must be appointed where applicable and must enforce all security requirements implemented by the ADPSO or ADPSSO for remote terminal areas. TASOs must ensure that all countermeasures required to protect the remote areas are in place. The TASOs must be appointed according to the physical location of the terminals.

(d) The ATASO may be appointed to support the TASOs when the number of terminals exceeds the required reasonable quantity or are outside the visible area of the TASO.

(e) An NSO is appointed, in writing, by the CO or OIC for each system of networked computers for which the command is sponsor. The NSO is in some respects the ADPSSO for an assigned network and responsible to the command ADPSO.

8. Action

a. MED-09D must operate and maintain the BUMED AIS Security Program.

b. Naval Medical Department activities must establish an AIS security program.

c. Naval Medical Department activities must complete their activity accreditation documentation per reference (a).

d. All personnel using BUMED AIS equipment, systems, and data or communicating with equipment must comply with this instruction.

9. Reports Exemption. Reporting requirements contained in this instruction are exempt from reports control per reference (k) part IV, G11 and G15.

D. F. HAGEN

Distribution:
All Internal BUMED Codes
SNDL, C28G (BRDENCLINIC)
C28H (BRMEDCLINIC)
C31J (BRMEDCLINIC)
C31K (NAVMEDADMINU)
C34F (BRMEDCLINIC and NAVMEDCLINIC LONDON DET)
C34G (BRDENCLINIC)
C52 (BUMED SHORE BASED DETACHMENTS)
C58Q (BRMEDCLINIC)
C58R (BRDENCLINIC)
C85A (BRMEDCLINIC)
FA47 (NAVHOSP)
FA48 (NAVDENCEN)
FA49 (NAVMEDCLINIC)
FB58 (NAVHOSP)
FB59 (NAVDENCEN)
FB60 (NAVMEDCLINIC)
FC16 (NAVMEDCLINIC)
FC17 (NAVHOSP)
FC18 (NAVDENCEN)
FF72 (NAVMEDCLINIC)
FH (BUMED COMMAND ACTIVITIES)
FT108 (NAVHOSP)
FT109 (NAVDENCEN)
FT110 (NAVMEDCLINIC)
FW1 (NATNAVMEDCEN)
FW2 (NATNAVDENCEN)
FW3 (NAVHOSP)
FW4 (NAVMEDCLINIC)

Copy to:
SNDL, 21A (CINCS)
23A2 (COMNAVFORJAPAN, COMNAVMARIANAS only)
28C2 (COMNAVSUFGRU LONG BEACH only)
28K1 (COMSUBGRU TWO only)
42A1 (COMFAIRCARIB, COMFAIRKEFLAVIK)
42A3 (COMFAIRMED)
42B1 (COMHELWINGSLANT only)
42B2 (COMMATVAQWINGPAC, COMPATWINGSPAC only)

Copy to: (continued)
SNDL, FA6 (NAS KEY WEST only)
FA24 (COMNAVBASE CHARLESTON, GUANTANAMO BAY, NORFOLK, and PHILADELPHIA only)
FB28 (COMNAVBASE PEARL HARBOR, SAN DIEGO, SAN FRANCISCO, SEATTLE only)
FB50 (COMUSFAC)
FC3 (COMNAVACT UK only)
FF1 (COMNAVDIST)
FF38 (USNA)
FKR3C (NAVAIRTESTCEN)
FT1 (CNET)
FT2 (CNATRA)
FT5 (CNTECHTRA)
FT28 (NETC)
FT31 (NTC GREAT LAKES, ORLANDO only)
V3 (COMCABEAST only)
V8 (CG MCRD PARRIS ISLAND only)
V12 (MCCDC QUANTICO)
V16 (CG MCB CAMP BUTLER, CAMP LEJEUNE, and CAMP PENDLETON only)

Stocked:
Naval Aviation Supply Office
Physical Distribution Division Code 103
5801 Tabor Ave.
Phila., PA 19120-5099

DEFINITIONS

1. Administrative Security. The management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data.

2. AIS Resources. All AIS equipment, personnel, software, supplies, facilities, and data used to support an automated process or function.

3. AAISSP. Activity Automated Information Systems Security Plan.

4. Call Back. A procedure for positively identifying a user and terminal dialing into a computer system by disconnecting the calling terminal and reestablishing the connection by the computer system's dialing the telephone number of the calling terminal.

5. Cost-Risk Analysis. The assessment of the costs of a potential risk of loss or compromise of data in an AIS or network without data protection vice the cost of providing data protection.

6. Data Dependent Protection. The protection of data at a level commensurate with the sensitivity level of the individual data elements rather than with the sensitivity of the entire file which includes the data elements.

7. Emanation Signals. Incidental electromagnetic and acoustic emanations which are transmitted as radiation through air and conductors.

8. Embedded Computers. Microprocessors, installed in non-AIS equipment that are integral to the functional operation of equipment which possess at a maximum a keypad for which data to establish parameters is input. The microprocessor is designed to perform a specific function or functions and is not programmable.

9. FIRMR. Federal Information Resources Management Regulation.

10. Network Security. The protection that results from all measures designed to prevent deliberate, inadvertent, or unauthorized disclosure, acquisition, manipulation, or modification of information in a network.

11. Privacy Protection. Involves the establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of data records and to protect both security and confidentiality against any anticipated

threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained.

12. Risk Analysis. An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

13. TEMPEST. The unclassified term referring to incidental electromagnetic and acoustic emanations which are extremely vulnerable to collection and intelligence processing.